# WHO GETS ACCESS?

## PROTECTING COMPANY DATA WITHOUT FRUSTRATING YOUR EMPLOYEES AND INCREASING COST

STRONGER SECURITY

BETTER EXPERIENCE

LOWER COST

SMARTER DECISIONS

FUTURE-READY

---

A PRACTICAL PLAYBOOK FOR REAL PROBLEMS. REAL SOLUTIONS. MEASURABLE IMPACT.

WRITTEN BY

**RAAVI BHATKAR**

# WHO GETS ACCESS

Protecting company data without frustrating your employees and increasing cost

**Written by Raavi Bhatkar**

# Introduction

Mid-sized companies migrating from legacy authentication systems repeatedly make poor trade-offs between security, usability, and operational cost.

The mistake is treating authentication as a simple technology replacement project. Authentication sits at the intersection of security, employee productivity, customer experience, IT operations, legacy infrastructure, compliance, and cost.

> *The goal is not to choose the most technology. The goal is to make the right trade-off for each user, system, and level of risk.*

# 1. Stop Optimizing Authentication in Isolation

A migration should not begin with: **Which authentication technology should we buy?**

It should begin with: **What authentication problems are we trying to solve for each type of user and system?**

Office employees, administrators, customers, shared-workstation operators, legacy applications, and service accounts do not have identical needs. One authentication method should not automatically be forced onto every environment.

# 2. The Three-Way Trade-Off

**Security:** How difficult is it for an attacker to gain unauthorized access?

**Usability:** How much friction does authentication create for legitimate users?

**Operational Cost:** How much infrastructure, support, recovery, training, and administration is required?

The goal is to find the best acceptable balance between all three.

> *A control that users constantly work around is not as secure as it looks on paper.*

# 3. Classify Users Before Choosing Technology

**Privileged Users:** Use phishing-resistant authentication, strong MFA, tighter session controls, enhanced monitoring, and carefully designed recovery.

**Standard Employees:** Prioritize SSO, sensible MFA, passwordless options where practical, and low-friction recovery.

**Shared Workstation Users:** Factories, logistics operations, call centres, and shift-based teams often share terminals and move between stations. Consider fast account switching, short-lived sessions, managed PIN mechanisms, badge-based identity, and device trust combined with individual authentication.

**Customers:** Use progressive authentication and increase verification when the risk or value of the action increases.

## 4. Never Replace Everything at Once

A big-bang migration creates unnecessary business risk. Use a staged approach instead.

**Phase 1 — Create an Identity Inventory:** Document applications, authentication protocols, user directories, service accounts, shared accounts, external identity providers, and MFA mechanisms.

**Phase 2 — Build a Compatibility Layer:** Support modern standards while allowing controlled, temporary integration with legacy systems where necessary.

**Phase 3 — Migrate by Risk and Feasibility:** Prioritize applications using **Risk × Usage × Migration Feasibility**.

## 5. Passwordless Is Not Automatically Operationally Simple

Passwordless authentication can improve resistance to phishing, but deployment decisions must consider reality.

Ask what happens when a device is lost, a workstation is shared, a user changes devices, hardware fails, or recovery is needed.

> *A secure login method with a weak recovery process is still a weak identity system.*

## 6. Treat Recovery as Part of Authentication

Many organizations secure the login path and then create an easy bypass through helpdesk recovery. Attackers will target the weaker path.

Recovery should use appropriate identity verification, stronger controls for high-risk accounts, audit logging, fraud detection, and additional approval where justified.

The easiest way into an account should not be the recovery process.

## 7. Avoid the MFA-Everywhere, Every-Time Trap

More prompts do not automatically mean more security. Excessive prompts create fatigue, mistakes, frustration, and lower productivity.

Use context where appropriate: trusted devices, unusual location changes, anomalous behaviour, privileged actions, and transaction risk.

> *Authentication should become stronger when risk increases—not simply become repetitive for everyone.*

## 8. Shared Accounts Are Usually an Identity Design Problem

Legacy systems often rely on shared credentials because they are operationally convenient. Simply banning them without providing a fast alternative often causes workarounds.

Replace shared accountability gaps with individual identities, fast login methods, quick switching, short sessions, and role-based access.

## 9. Separate Human and Machine Authentication

Service accounts and workloads should not be treated like employees.

Avoid permanent passwords embedded in scripts. Prefer managed identities, short-lived credentials, certificate-based authentication where appropriate, secret rotation, and workload identity approaches.

## 10. Measure Authentication Like a Business System

**Security Metrics:** Account takeover attempts, MFA bypass attempts, privileged authentication anomalies, and suspicious recovery activity.

**Usability Metrics:** Average login time, authentication abandonment, MFA prompt frequency, and account recovery frequency.

**Operational Metrics:** Password-reset tickets, authentication-related helpdesk cost, application integration time, and identity platform reliability.

If security improves but helpdesk demand triples and employees adopt workarounds, the migration is not yet successful.

## 11. The Five-Question Decision Framework

**1. What threat are we solving?** Be specific.

**2. Who will use it?** Administrators and warehouse operators are different populations.

**3. What environment exists?** Personal laptop, mobile device, shared terminal, or unmanaged endpoint?

**4. What happens when it fails?** Authentication should fail safely without unnecessarily stopping the business.

**5. What is the recovery path?** If recovery is weak, the apparent strength of login controls may be irrelevant.

# Final Principle

The best authentication architecture is not the one with the most technology.

For mid-sized companies, the winning strategy is usually a carefully staged migration that understands different user environments, removes legacy risk gradually, uses modern standards, protects recovery processes, reduces unnecessary friction, and measures both security and operational outcomes.

**Authentication should become stronger without becoming the reason people cannot do their jobs.**

> *It is the one where security controls are strong enough to resist realistic threats, simple enough for legitimate users to follow, and practical enough for the organization to operate reliably.*

## Need help with your authentication or identity strategy?

I provide practical consultation to help your business make better security, usability, and cost decisions.

**raavi.munaf@gmail.com**

Raavi Bhatkar